

~~CONFIDENTIAL~~

ICS REGISTRY

The Director of Central Intelligence

Washington, D.C. 20505

Intelligence Community Staff

IC/83/3375  
25 April 1983

MEMORANDUM FOR: Senior Interagency Group (Intelligence)

FROM:

  
Executive Secretary, SIG(I)

SUBJECT:

Proposed NSDD--National Policy for Operations  
Security

*Conte 24*

25X1

1. The attached is in response to action called for at the SIG(I) meeting of 11 March 1983, that the proposed NSDD for NSC issuance on operations security be put into final form. It is submitted for your personal review.

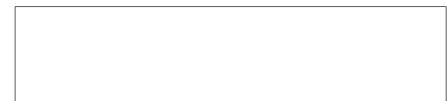
2. Unless you have provided your comments by noon, 2 May 1983, or have requested more time for consideration, the Executive Secretary will take it that you concur in the draft proposal to be forwarded for the Chairman's approval.



25X1  
25X1

Attachment:  
As Stated

Distribution:  
Assistant to the President  
for National Security Affairs  
Deputy Secretary of State  
Deputy Secretary of Defense  
Attorney General  
Chairman, Joint Chiefs of Staff



25X1

~~CONFIDENTIAL~~

Distribution

IC/83/3375

Office of the Vice President (Don Gregg)

NSC (W. Hall)

Department of State (L. Paul Bremer)

Department of Defense (LTC Rick Higgins)

Department of Justice (Mary Lawton)

Joint Chiefs of Staff (Lt Gen Paul Gorman)

D/FBI

D/NSA

D/DIA

C/IG/CM (Gen Stilwell)

DCI

DDCI

CIA (C. Briggs)

DCI/SA

STAT

Executive Secretariat (T. Cormack)

Executive Registry

D/ICS

IG/WG

STAT

SIG(I) Chrono

SIG(I) Subject

Secretariat Staff Registry

ICS Registry

**CONFIDENTIAL**

**Interagency Group/Countermeasures**

Washington, D.C. 20505

14 APR 1983

MEMORANDUM FOR THE CHAIRMAN, SENIOR INTERAGENCY GROUP/INTELLIGENCE

SUBJECT: National Policy for Operations Security [REDACTED]

25X1

[REDACTED] each department and agency that undertakes operations or activities that are classified, or otherwise valuable to hostile intelligence, should establish an internal operations security program.

25X1

[REDACTED] The Interagency Group/Countermeasures (IG/CM) has developed a response to that need (TAB A), which we recommend for SIG-I approval and promulgation as national policy.

25X1

[REDACTED] There is consensus that such a policy is needed. There is also a consensus that operations security programs must be highly flexible and adapted to specific missions. For this reason, the proposed Operations Security Advisory Committee need not be given directive authority, rather, it should provide recommendations and advice as requested. It should also serve to coordinate those operations security matters cutting across department lines.

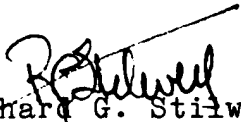
25X1

[REDACTED] At the SIG/I meeting of 11 March 83, it was agreed that the proposed national policy on operations security be put into final form, incorporating comments on the draft proposal. This has now been done, and the revised proposal circulated.

25X1

[REDACTED] Accordingly, it is recommended that the proposed issuance at TAB A be forwarded to the members of the SIG-I, for their consideration. At TAB B is a proposed transmittal for this purpose.

25X1

  
Richard G. Stilwell  
General, USA (Ret.)  
Chairman, IG/CM

Enclosures

**CONFIDENTIAL**

25X1

PROPOSED NSDD

NATIONAL POLICY FOR OPERATIONS SECURITY

1. Policy. The national security requires that all prudent and lawful measures be taken to deny adversaries information concerning sensitive activities undertaken by the United States Government. Such protective measures shall include an analysis of such activities to determine whether indicators exist that are available to, or readily observable by, adversaries, which, taken separately or in the aggregate, tend to reveal or confirm the existence and/or nature of such activities. Once such indicators have been identified, appropriate actions shall be taken to ensure that such vulnerabilities are eliminated or minimized.
2. Implementation. Each department and agency of the United States that conducts sensitive activities, as defined herein, shall adopt internal policies and procedures designed to accomplish the objectives set forth in paragraph 1. These policies shall ensure the protection of their resources and activities, balancing mission effectiveness and security needs with practical cost considerations.
3. Coordination. There is hereby established as a permanent subcommittee of the Interagency Group/Countermeasures, an Operations Security Advisory Committee, chaired by a representative of the Secretary of Defense, with membership from each of the departments and agencies participating in the IG/CM. Other departments and agencies may be invited to meetings of the Committee by the Chairman. The Committee does not have directive authority over departments and agencies of the executive branch. The functions of the Committee will be to:
  - a. Prepare general OPSEC documents for use as appropriate by agencies of the executive branch;
  - b. Develop, as requested, recommendations with respect to specific operations security measures applicable to the executive branch;
  - c. Provide recommendations to executive departments and agencies, as requested, concerning operations security vulnerabilities, and methods of correcting such deficiencies;
  - d. Coordinate support for operations security activities, as necessary, within the executive branch; and
  - e. Coordinate operations security corrective measures involving more than one department or agency, as requested.

4. Definitions. As used herein, the term -

a. "Operations Security (OPSEC)" refers to the process intended to deny information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and execution of government activities. Application of OPSEC involves a process of analysis of a program, project, or office, to determine needed security modifications that will result in adequate protection. By its very nature, OPSEC is program specific, and produces a highly tailored, flexible approach to security.

b. "Sensitive activities" refers to operations, investigations, inquiries, tests, research, training, exercises, and other functions of departments and agencies, or their contractors, the disclosure of which to adversaries could reasonably be expected to damage the national security.

c. "Indicators" refers to those characteristics or qualities of sensitive activities -- ordinarily unclassified -- that exposes them, or makes them more comprehensible, either wholly or in part, to adversaries. These characteristics or qualities are ordinarily necessary to the performance of, necessarily attendant to, or the consequence of, a sensitive activity.

MEMORANDUM FOR MEMBERS OF THE SIG/I

SUBJECT: National Policy for Operations Security

At the 11 March 83 meeting of the SIG/I, it was agreed that the proposed NSC issuance on operations security be put into final form, incorporating comments provided by SIG/I members as necessary. This has now been done, and the revised paper is at TAB A. I would appreciate your consideration of this paper. Please advise me of your views by \_\_\_\_\_.

*see Registry*

The Director of Central Intelligence

Washington, D.C. 20505

Intelligence Community Staff

IC/83/3375  
25 April 1983

MEMORANDUM FOR: Senior Interagency Group (Intelligence)

FROM:

  
Executive Secretary, SIG(I)

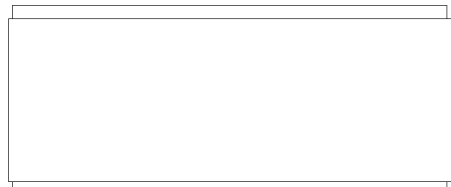
25X1

SUBJECT:

Proposed NSDD--National Policy for Operations  
Security

1. The attached is in response to action called for at the SIG(I) meeting of 11 March 1983, that the proposed NSDD for NSC issuance on operations security be put into final form. It is submitted for your personal review.

2. Unless you have provided your comments by noon, 2 May 1983, or have requested more time for consideration, the Executive Secretary will take it that you concur in the draft proposal to be forwarded for the Chairman's approval.



25X1

Attachment:  
As Stated

Distribution:  
Assistant to the President  
for National Security Affairs  
Deputy Secretary of State  
Deputy Secretary of Defense  
Attorney General  
Chairman, Joint Chiefs of Staff



25X1

CONFIDENTIAL

Distribution

IC/83/3375

Office of the Vice President (Don Gregg)

NSC (W. Hall)

Department of State (L. Paul Bremer)

Department of Defense (LTC Rick Higgins)

Department of Justice (Mary Lawton)

Joint Chiefs of Staff (Lt Gen Paul Gorman)

D/FBI

D/NSA

D/DIA

C/IG/CM (Gen Stilwell)

DCI

DDCI

CIA (C. Briggs)

DCI/SA [redacted]

Executive Secretariat (T. Cormack)

Executive Registry

D/ICS [redacted]

IG/WG [redacted]

SIG(I) Chrono

SIG(I) Subject

Secretariat Staff Registry

ICS Registry

STAT

STAT  
STAT



**CONFIDENTIAL**

**Interagency Group/Countermeasures**

Washington, D.C. 20505

14 APR 1983

MEMORANDUM FOR THE CHAIRMAN, SENIOR INTERAGENCY GROUP/INTELLIGENCE

SUBJECT: National Policy for Operations Security

25X1

each department and agency that undertakes operations or activities that are classified, or otherwise valuable to hostile intelligence, should establish an internal operations security program.

25X1

The Interagency Group/Countermeasures (IG/CM) has developed a response to that need (TAB A), which we recommend for SIG-I approval and promulgation as national policy.

25X1

There is consensus that such a policy is needed. There is also a consensus that operations security programs must be highly flexible and adapted to specific missions. For this reason, the proposed Operations Security Advisory Committee need not be given directive authority, rather, it should provide recommendations and advice as requested. It should also serve to coordinate those operations security matters cutting across department lines.


25X1

At the SIG/I meeting of 11 March 83, it was agreed that the proposed national policy on operations security be put into final form, incorporating comments on the draft proposal. This has now been done, and the revised proposal circulated.

25X1

Accordingly, it is recommended that the proposed issuance at TAB A be forwarded to the members of the SIG-I, for their consideration. At TAB B is a proposed transmittal for this purpose.

25X1

  
Richard G. Stilwell  
General, USA (Ret.)  
Chairman, IG/CM

Enclosures

**CONFIDENTIAL**

25X1

PROPOSED NSDD

NATIONAL POLICY FOR OPERATIONS SECURITY

1. Policy. The national security requires that all prudent and lawful measures be taken to deny adversaries information concerning sensitive activities undertaken by the United States Government. Such protective measures shall include an analysis of such activities to determine whether indicators exist that are available to, or readily observable by, adversaries, which, taken separately or in the aggregate, tend to reveal or confirm the existence and/or nature of such activities. Once such indicators have been identified, appropriate actions shall be taken to ensure that such vulnerabilities are eliminated or minimized.
2. Implementation. Each department and agency of the United States that conducts sensitive activities, as defined herein, shall adopt internal policies and procedures designed to accomplish the objectives set forth in paragraph 1. These policies shall ensure the protection of their resources and activities, balancing mission effectiveness and security needs with practical cost considerations.
3. Coordination. There is hereby established as a permanent subcommittee of the Interagency Group/Countermeasures, an Operations Security Advisory Committee, chaired by a representative of the Secretary of Defense, with membership from each of the departments and agencies participating in the IG/CM. Other departments and agencies may be invited to meetings of the Committee by the Chairman. The Committee does not have directive authority over departments and agencies of the executive branch. The functions of the Committee will be to:
  - a. Prepare general OPSEC documents for use as appropriate by agencies of the executive branch;
  - b. Develop, as requested, recommendations with respect to specific operations security measures applicable to the executive branch;
  - c. Provide recommendations to executive departments and agencies, as requested, concerning operations security vulnerabilities, and methods of correcting such deficiencies;
  - d. Coordinate support for operations security activities, as necessary, within the executive branch; and
  - e. Coordinate operations security corrective measures involving more than one department or agency, as requested.

4. Definitions. As used herein, the term -

a. "Operations Security (OPSEC)" refers to the process intended to deny information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and execution of government activities. Application of OPSEC involves a process of analysis of a program, project, or office, to determine needed security modifications that will result in adequate protection. By its very nature, OPSEC is program specific, and produces a highly tailored, flexible approach to security.

b. "Sensitive activities" refers to operations, investigations, inquiries, tests, research, training, exercises, and other functions of departments and agencies, or their contractors, the disclosure of which to adversaries could reasonably be expected to damage the national security.

c. "Indicators" refers to those characteristics or qualities of sensitive activities -- ordinarily unclassified -- that exposes them, or makes them more comprehensible, either wholly or in part, to adversaries. These characteristics or qualities are ordinarily necessary to the performance of, necessarily attendant to, or the consequence of, a sensitive activity.

MEMORANDUM FOR MEMBERS OF THE SIG/I

SUBJECT: National Policy for Operations Security

At the 11 March 83 meeting of the SIG/I, it was agreed that the proposed NSC issuance on operations security be put into final form, incorporating comments provided by SIG/I members as necessary. This has now been done, and the revised paper is at TAB A. I would appreciate your consideration of this paper. Please advise me of your views by \_\_\_\_\_.